

REMARKS

Applicant's invention relates to a time-stamping protocol for time-stamping digital documents. An outside agency (e.g., a time-stamping authority - TSA) receives identifying data associated with a document from the document owner, for example, and creates a multi-part receipt. This identifying data may be a hash value of the document. The TSA creates a first receipt based on the identifying data and a linking value (e.g., a unique nonce). The TSA also creates a second receipt based on the same linking value used to create the first receipt, and a time indication. Finally, the TSA certifies both the first and second receipts using a cryptographic signature scheme, such as a private key, and transmits the certifications to the owner.

Applicant respectfully traverses the rejection of claim 1 under 35 U.S.C. § 102(b) as being anticipated by Haber et. al. (U.S. Patent No. Re. 34,954). Claim 1 explicitly requires, "creating at said outside agency a first receipt based on said identifying data and a linking value . . . [and] . . . creating at said outside agency a second receipt based on said linking value and a time indication." In other words, claim 1 requires that the outside agency create both the first and the second multi-part receipts, and further, that both receipts are based at least in part on the same linking value. Possession of only one of the receipts is not sufficient for verifying the date of the document. The user must possess both the first and second parts receipts to verify the date of the document. Because both receipts comprise the linking value (e.g., a unique, randomly chosen nonce), the date or time of the document may be verified by comparing the linking value of the first receipt with the linking value of the second receipt. If the two linking values are the same, the date and/or time of the document is verified.

The patent to Haber does not teach that the TSA creates a multi-part receipt based on the same linking value as required by claim 1. Rather, the time stamping task is specifically distributed among the plurality of randomly chosen agents to negate the need for a linking value in each of the receipts. In Haber, the TSA (or author/requestor) transmits the document to a

predetermined number (i.e., a plurality) of randomly chosen agents. Upon receipt of the document, each agent creates a separate receipt and returns it to the TSA (or author/requestor). Each of the randomly chosen agents creates their separate receipt individually and independently of the other agents.

Because each agent generates their receipt individually and independently of the other agents, the date of the document in Haber may be verified using any one of the independently created receipts. Indeed, comparison of any of the values in one receipt with any of the values in another receipt to verify the date or time of the document are neither needed nor desired.

This is because independent verification is the fundamental goal of the patent of Haber.

Applicants respectfully direct the Examiner's attention to column 4 of Haber, lines 46-59, which reveal that distributing the time-stamping task (i.e., independent generation) substantially minimizes the chance that an author, in collusion with the stamping agency, would be able to falsify a receipt. The agents in Haber have no need for a linking value as required by claim 1.

Simply put, Haber never discloses a linking value that links a time value in one receipt to identifying data in a different receipt. The Examiner admits this fact, but theorizes that a linking value must exist in Haber (i.e., it is inherent) because Haber discloses combining the receipts received from the agents. The Examiner cites column 5 of Haber, lines 9-15 for support.

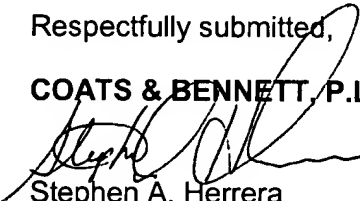
Respectfully, the Examiner appears to have misconstrued this passage. According to the cited passage, the TSA simply collects each of the independently generated receipts received from the predetermined number of agents together. Each of the receipts received from the agents may or may not be certified by the TSA using a cryptographic signature scheme. However, each of the receipts is still independent of one another, regardless of how or where they are collected. None of the receipts comprise the requisite linking value. In this case, the TSA in Haber acts simply as an administrative entity that permits the author/requestor to escrow the receipts.

Finally, the Examiner's theory of inherency in Haber simply does not comport to the teachings of Haber. Even Haber considers the distribution (and thus, the independent generation and verification) of the time-stamping task to provide "advantages over the receipt linking procedure." *Haber*, col. 5, ll. 16-21. Simply put, the patent to Haber fails to teach, "creating at said outside agency a first receipt based on said identifying data and a linking value . . . [and] . . . creating at said outside agency a second receipt based on said linking value and a time indication," and thus, cannot anticipate claim 1 as a matter of law. Accordingly, Applicant respectfully requests the allowance of claim 1, and its dependent claims 2-8.

The Examiner also rejected claim 9 under 35 U.S.C. § 102(b) as being anticipated by Haber, citing the same reasons as those cited above with respect to claim 1. However, claim 9 contains language similar to that of claim 1 above. Therefore, for reasons similar to those stated above, the patent to Haber fails to anticipate claim 9 under § 102 as a matter of law. Accordingly, Applicant respectfully requests the allowance of claim 9, and its dependent claims 10-19.

Dated: January 23, 2004

By:

Respectfully submitted,
COATS & BENNETT, P.L.L.C.

Stephen A. Herrera
Registration No. 47,642

P.O. Box 5
Raleigh, NC 27602
Telephone: (919) 854-1844